Cascadia Intellectual Property
500 Union Street, Suite 1005
Seattle, Washington 98101
Telephone: (206) 381-3900
Facsimile: (206) 381-3999

RECEIVED
CENTRAL FAX CENTER
MAY - 2 2007

Facsimile Transmittal

To:	Board of Patent Appeals and Interferences	**Fax:**	(571) 273-8300
From:	Krista A. Wittman KAW	**Date:**	May 2, 2007
Re:	U.S. Patent Application Serial No. 09/346,559	**Pages:**	26 (including cover sheet)
CC:			

☐ Urgent ☐ For Review ☐ Please Comment ☐ Please Reply ☐ Please Recycle

Notes: Regarding the above-identified U.S. Patent Application, please find attached hereto:

- USPTO Transmittal Form
- Reply Brief

This Reply Brief was also sent to the Board of Patent Appeals and Interferences at (571) 273-0053. Please disregard the duplicate copy. Thank you.

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM (to be used for all correspondence after initial filing)		
	Application Number	09/346,559
	Filing Date	June 30, 1999
	First Named Inventor	Goldberg, David
	Art Unit	2625
	Examiner Name	James A. Thompson
Total Number of Pages in This Submission	Attorney Docket Number	D/99176

RECEIVED
CENTRAL FAX CENTER
MAY - 2 2007

ENCLOSURES *(Check all that apply)*

- [ ] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ________
  - [ ] Landscape Table on CD
- [ ] After Allowance communication to (TC)
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [x] Other Enclosure(s) (please identify below):

Facsimile Cover Sheet

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Cascadia Intellectual Property		
Signature	Krista Wittman		
Printed name	Krista A. Wittman		
Date	May 2, 2007	Reg. No.	59,594

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	L. Liparteliani		
Typed or printed name	Lali Liparteliani	Date	May 2, 2007

Reply Brief
Docket No. D/99RECEIVED
CENTRAL FAX CENTER
MAY - 2 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of Goldberg et al.	Group Art Unit: 2625
Serial No.: 09/346,559	Examiner: James A. Thompson
Filed: July 30, 1999	
For: System For Authenticating Hardcopy Documents	

REPLY BRIEF

Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF ON BEHALF OF GOLDBERG ET AL.:

Appellant appeals from the Office Action mailed, June 5, 2006, in which currently-pending claims 1-23 stand rejected. Appellant filed a Notice of Appeal with a one-month extension of time by facsimile on September 14, 2006 and an Appeal Brief on November 14, 2006. An Examiner's Answer was mailed on March 2, 2007. This Reply Brief is submitted in response to the Examiner's Answer, pursuant to 37 C.F.R. § 41.41(a)(1).

TABLE OF CONTENTS

1. STATUS OF CLAIMS

Rejected Claims 1-23 are pending and are the subject of this Reply Brief. The claims involved in this appeal are included in Appendix 4.

2. GROUNDS FOR REJECTION TO BE REVIEWED ON APPEAL

A. Issue I

Whether Claims 1-3, 5, 7-8, 12-13, and 21-23 stand properly rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,898,779, issued to Squilla et al. ("Squilla").

B. Issue II

Whether Claim 4 stands properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Squilla in view of U.S. Patent No. 5,157,726, issued to Merkle et al. ("Merkle").

C. Issue III

Whether Claims 6 and 9-11 stand properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Squilla in view of U.S. Patent No. 5,946,103, issued to Curry.

D. Issue IV

Whether Claims 14-17 stand properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Squilla in view of U.S. Patent No. 5,486,686, issued to Zdybel et al. ("Zdybel").

E. Issue V

Whether Claims 18-20 stand properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Squilla in view of U.S. Patent No. 6,111,953, issued to Walker et al. ("Walker").

3. CLARIFYING ARGUMENTS

This Reply Brief presents clarifying remarks in rebuttal to the Examiner's Answer.

A. U.S. Patent No. 5,898,779 ("Squilla")

1. Claims 1-3, 5, 7-8, and 12-13 (Group I)

The issue is not whether Squilla discloses a scanned representation of a hardcopy document. Rather, the primary distinction between Squilla and independent Claim 1 is the arranging in the memory the scanned representation of a hardcopy document *for rendering* at a printer a signed and authenticated hardcopy document, which applicant continues to assert is neither taught nor suggested by Squilla.

Claim 1 recites arranging in a memory a scanned representation of a hardcopy document with a digital encoding of an authentication token for rendering at a printer a *signed and authenticated hardcopy* document. An original hardcopy document is scanned and recorded as grayscale image data (Spec., p. 6, lines 16-18). The recorded data is sent to a compression module for lossy compression (Spec., p. 6, lines 24-25) and a halftone generator for creating halftone image data of the complete document (Spec., p. 7, lines 11-12). An authentication token generator receives the compressed image data and produces an authentication token, including a compressed representation of the original hardcopy document and means for authenticating the document (Spec., p. 7, lines 20-25). An encoding module receives the authentication token and halftone image data to produce encoded halftone image data for rendering a signed and authenticated hardcopy document at a printer (Spec., p. 8, lines 17-19). The signed document is a *complete* copy for rendering as a hardcopy of the original hardcopy document that has been authenticated by the authentication token.

In contrast, Squilla primarily focuses on authenticating digital images, particularly digital photographs, in *electronic* form using a digital camera. Digital cameras have a finite amount of battery power, and minimizing the amount of

battery power used during an operation is desirable (Squilla, Col. 2, lines 49-56). A major drawback of using a digital camera for image authentication is that the camera generates a digital hash from the whole image, which requires large amounts of battery power (Squilla, Col. 2, lines 61-63). The authentication system of Squilla minimizes battery power usage during image authentication by selecting a region of interest within a complete image for generating a digital signature (Squilla, Col. 2, lines 63-67; Col. 4, lines 13-19; and Col. 8, lines 35-40). To further conserve the digital camera battery, Squilla teaches processing a region of interest, rather than the complete image, using a FlashPix™ application (Col. 8, lines 56-58).

The FlashPix™ file contains a complete image and several lower resolution copies, which are each divided into rectangular tiles (Squilla, Col. 8, lines 56-62). Each tile has a distinct autonomy and can be processed separately from the other tiles (Squilla, Col. 8, lines 62-64). A user can access, display, or print a region of interest from the complete image by selecting rectangular tiles with portions of the desired image contained within the tiles (Squilla, Col. 8, lines 58-62). The printed image of Squilla includes tiles from a complete digital image, selected by a user. Therefore, Squilla fails to suggest or disclose an *authenticated* printed image with a *digital signature*. Squilla further fails to teach arranging in a memory a scanned representation of a hardcopy document for rendering at a printer a *complete* signed and authenticated hardcopy document, per Claim 1.

Claim 1 also recites arranging in the memory a scanned representation of the hardcopy document with a *digital encoding* of the authentication token for rendering at a printer the signed and authenticated hardcopy document. In particular, an encoding module receives the authentication token from an authentication token generator and produces encoded halftone image data, which is used by a printer to render the signed hardcopy document (Spec., p. 8, lines 17-19). The authentication token is encoded using embedded data, including a halftone pattern (Spec., p. 8, lines 19-21). In contrast, Squilla teaches creating a digital signature by selecting a region of interest from an image, compressing the region of interest, creating a hash of the compressed region of interest, and

encrypting the hash using a private key (Squilla, Col. 8, lines 34-51; FIGURE 7). The digital signature is appended to a digital image file for storing with the unaltered digital image (Squilla, Col. 7, lines 49-58). Therefore, Squilla fails to teach an additional step of encoding the compressed, hashed, and encrypted image data, per Claim 1.

Moreover, Claim 1 recites an authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data (Spec., p. 8, lines 1-6). In contrast, Squilla teaches compressing a selected region of a digital image, hashing the compressed region, and encrypting the hash to generate a digital signature (Squilla, Col. 8, lines 34-51). The digital signature includes a hash of the region of interest and photographer's information, such as the time and date of the photograph, which is attached to the hashed region of interest (Squilla, Col. 7, lines 31-34; Col. 8, lines 34-51). Therefore, Squilla teaches a digital signature, which includes a hash of the compressed image data, rather than unhashed encrypted image data. Squilla further differs from Claim 1 by failing to teach or suggest a digital signature in which the hash of the compressed image data includes both the compressed image data and a hash of the compressed image data.

Accordingly, a *prima facie* case of anticipation under 35 U.S.C. § 102(e) has not been shown. Claims 2-3, 5, 7-8, and 12-13 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Applicant continues to assert that Squilla fails to anticipate Claims 2 and 3, not only on each claim's dependency on independent Claim 1, but also based on the subject matter of the claims themselves. Claim 2 recites recording a *scanned representation* of the signed hardcopy document. The scanned representation of the signed hardcopy doucment is recorded to create a digital representation of the document data for verifying the authenticity of the hardcopy document (Spec., p. 11, lines 4-13). In contrast, Squilla teaches applying a verification process to a digital signature, which is stored as a digital representation (Col. 8, lines 50-51), rather than a hardcopy document. Therefore,

Squilla fails to teach a verification process that includes recording a *scanned representation* of the signed hardcopy document, per dependent Claim 2.

Further, Claim 3 recites *visually comparing* the signed hardcopy document with the authenticated lossy compressed image data. In contrast, Squilla teaches a system, which separates a digital signature from a digital image, decrypts the digital signature to obtain an original hash, identifies regions of interest from the digital image, creates a new hash of the region of interest, and compares the new hash with the original hash (Squilla, Col. 7, line 59-Col.8, line 16). The system compares the hashes for determining whether the selected portion of the image has been altered (Squilla, Col. 8, lines 9-19). Therefore, Squilla teaches an authentication system for comparing an original hash and a new hash, rather than *visually comparing* a signed *hardcopy* document with authenticated lossy compressed *image data*.

Moreover, Squilla differs from Claims 2 and 3 in other key aspects, such as the type and amount of data that is being authenticated. As described above, Squilla teaches verifying the authenticity of a digital image by separating a digital signature from the digital file, decrypting the digital signature to obtain the original hash, creating a new hash of the same region of interest, and comparing the decrypted hash with the new hash (Squilla, Col. 7, line 59-Col. 8, line 16). In contrast, Claim 2 recites recording a scanned representation of the signed hardcopy document, decoding the authentication token, decompressing the image data, and comparing the signed hardcopy document with the authenticated lossy compressed image data (Spec., p. 11, line 6-p. 12, line 21). Claim 3 recites visually comparing the signed hardcopy document with the authenticated lossy compressed image data. Thus, Squilla focuses on verifying the authenticity of a portion of a digital image, rather than a complete signed hardcopy document, which is based on an original hardcopy document.

Squilla also differs from dependent Claim 7, which recites encoding the authentication token in embedded data, and dependent Claim 8, which recites encoding the authentication token in a halftone pattern. As described above, Squilla teaches compressing, hashing, and encrypting a select portion of the

digital image (Col. 8, lines 44-47) without including an *additional* step of *encoding* the hashed data, per Claim 1. Therefore, Squilla fails to teach *encoding* a digital signature and further, fails to teach encoding a digital signature in *embedded data* or in a *halftone pattern*, per Claims 7 and 8.

Accordingly, the anticipation rejection cannot be sustained. As a *prima facie* case of anticipation has not been established, withdrawal of the rejection is respectfully requested.

II. Claims 21-23 (Group II)

The issue is not whether Squilla discloses a scanned representation of a hardcopy document. Rather, the primary distinction between Squilla and independent Claim 21 is the arranging in the memory the scanned representation of the hardcopy document *for rendering* at a printer a signed and authenticated hardcopy document.

Claim 21 recites arranging a scanned representation of a hardcopy document with a digital encoding of an authentication token for rendering at a printer a *signed and authenticated hardcopy* document. An original hardcopy document is scanned and recorded as grayscale image data (Spec., p. 6, lines 16-18). The recorded data is sent to a compression module for lossy compression (Spec., p. 6, lines 24-25) and a halftone generator for creating halftone image data of the complete document (Spec., p. 7, lines 11-12). An authentication token generator receives the compressed image data and produces an authentication token, including a compressed representation of the original hardcopy document and means for authenticating the document (Spec., p. 7, lines 20-25). An encoding module receives the authentication token and halftone image data to produce encoded halftone image data for rendering a signed and authenticated hardcopy document at a printer (Spec., p. 8, lines 17-19). The signed document is a *complete* copy for rendering as a hardcopy of the original hardcopy document that has been authenticated by the authentication token.

In contrast, Squilla primarily focuses on authenticating digital images, particularly digital photographs, in *electronic* form using a digital camera. Digital cameras have a finite amount of battery power, and minimizing the amount of

battery power used during an operation is desirable (Squilla, Col. 2, lines 49-56). A major drawback of using a digital camera for image authentication is that the camera generates a digital hash from the whole image, which requires large amounts of battery power (Squilla, Col. 2, lines 61-63). The authentication system of Squilla minimizes battery power usage during image authentication by selecting a region of interest within a complete image for generating a digital signature (Squilla, Col. 2, lines 63-67; Col. 4, lines 13-19; and Col. 8, lines 35-40). To further conserve the digital camera battery, Squilla teaches processing a region of interest, rather than the complete image, using a FlashPix™ application (Col. 8, lines 56-58).

The FlashPix™ file contains a complete image and several lower resolution copies, which are each divided into rectangular tiles (Squilla, Col. 8, lines 56-62). Each tile has a distinct autonomy and can be processed separately from the other tiles (Squilla, Col. 8, lines 62-64). A user can access, display, or print a region of interest from the complete image by selecting rectangular tiles with portions of the desired image contained within the tiles (Squilla, Col. 8, lines 58-62). The printed image of Squilla includes tiles from a complete digital image, selected by a user. Therefore, Squilla fails to suggest or disclose an *authenticated* printed image with a *digital signature*. Squilla further fails to teach arranging in a memory a scanned representation of a hardcopy document for rendering at a printer a *complete* signed and authenticated hardcopy document, per Claim 21.

Claim 21 also recites arranging a scanned representation of the hardcopy document with a *digital encoding* of the authentication token for rendering at a printer the signed and authenticated hardcopy document. In particular, an encoding module receives the authentication token from an authentication token generator and produces encoded halftone image data, which is used by a printer to render the signed hardcopy document (Spec., p. 8, lines 17-19). The authentication token is encoded using embedded data, including a halftone pattern (Spec., p. 8, lines 19-21). In contrast, Squilla teaches creating a digital signature by selecting a region of interest from an image, compressing the region of interest, creating a hash of the compressed region of interest, and encrypting the

hash using a private key (Squilla, Col. 8, lines 34-51; FIGURE 7). The digital signature is appended to a digital image file for storing with the unaltered digital image (Squilla, Col. 7, lines 49-58). Therefore, Squilla fails to teach an additional step of encoding the compressed, hashed, and encrypted image data, per Claim 21.

Moreover, Claim 21 recites an authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data (Spec., p. 8, lines 1-6). In contrast, Squilla teaches compressing a selected region of a digital image, hashing the compressed region, and encrypting the hash to generate a digital signature (Squilla, Col. 8, lines 34-51). The digital signature includes a hash of the region of interest and photographer's information, such as the time and date of the photograph, which is attached to the hashed region of interest (Squilla, Col. 7, lines 31-34; Col. 8, lines 34-51). Therefore, Squilla teaches a digital signature, which includes a hash of the compressed image data, rather than unhashed encrypted image data. Squilla further differs from Claim 21 by failing to teach or suggest a digital signature in which the hash of the compressed image data includes both the compressed image data and a hash of the compressed image data.

Accordingly, a *prima facie* case of anticipation under 35 U.S.C. § 102(e) has not been shown. Claims 22 and 23 are dependent on Claim 21 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Squilla differs from Claims 22 and 23 in key aspects, such as the type and amount of data that is being authenticated. As described above, Squilla teaches verifying the authenticity of a digital image by separating a digital signature from the digital file, decrypting the digital signature to obtain the original hash, creating a new hash of the same region of interest, and comparing the decrypted hash with the new hash (Squilla, Col. 7, line 59-Col. 8, line 16). In contrast, Claim 22 recites recording the signed hardcopy document, decoding the signed hardcopy document, decompressing the authenticated image data, and comparing the signed hardcopy document with the authenticated hardcopy

document (Spec., p. 11, line 6-p. 12, line 21). Thus, Squilla focuses on verifying the authenticity of a portion of a digital image, rather than a complete signed hardcopy document, which is based on an original hardcopy document.

Accordingly, the anticipation rejection cannot be sustained. As a *prima facie* case of anticipation has not been established, withdrawal of the rejection is respectfully requested.

B. U.S. Patent No. 5,157,726 ("Merkle")

Applicant continues to assert that the Squilla and Merkle references are being improperly combined, and the combination fails to disclose, teach, or suggest all the limitations of Claim 4.

Merkle teaches a system for authenticating a hardcopy document using a digital signature and a smart card (Merkle, Col. 4, lines 37-52). The output of the system is a digitally cleaned document that is an exact copy of the original document (Merkle, Col. 4, lines 18-23). In contrast, Squilla teaches selecting a region of interest from an image for use in a digital signature that is stored in a digital file with the unaltered image. A private key is used to subsequently verify that a particular photograph was taken on a particular camera (Squilla, Col. 7, lines 42-49).

One of ordinary skill in the art would not find a suggestion or motivation to combine Squilla with Merkle. Squilla teaches a system for generating and storing a digital signature in a digital image file, whereas Merkle teaches a system for printing a digitally cleaned hardcopy document. In particular, Squilla teaches an image format including a file header field with a location of the region of interest, a signature field with the digital signature, and a data field with the unaltered digital image (Squilla, Col. 5, lines 41-50). In contrast, Merkle teaches using a literal scanned representation of a hard copy document to print a digitally cleaned output document (Merkle, Col. 5, lines 36-41). Printing a digitally cleaned document is possible since the digital signature includes every significant piece of information in the document (Merkle, Col. 4, lines 42-46). The system of Merkle recovers the necessary data from the digital signature, which is digitally encoded and placed on the document, to print a clean version of the original

document (Merkle, Col. 5, lines 41-45).

Although, both references teach data authentication, Merkle focuses on data recovery and Squilla focuses on conserving battery power. The focus of Merkle and the focus of Squilla are contrasting since the digital signature in Merkle requires data from the whole document, and Squilla teaches a digital signature using only a portion of the document. Therefore, the Squilla and Merkle references are not in the same field of endeavor and should not be combined.

Further, the Squilla-Merkle combination fails to create a reasonable expectation of success. Squilla teaches selecting a region of interest from a digital image for creating a digital signature (Squilla, Col. 4, lines 13-22). In contrast, Merkle teaches creating a digitally cleaned hardcopy document from a signed hardcopy document (Merkle, Col. 5, lines 36-45). Combining the teachings of Squilla with the teachings of Merkle would thus provide, generating a digital signature from a selected region of interest and printing a digitally cleaned version of the document based only on the portion of the document contained in the digital signature. However, the selected portion of the document may not include all of the significant information necessary for recreating a digitally cleaned version of the whole document. As a result, the combination of Squilla and Merkle would not suggest to one of ordinary skill in the art that the combined process should be carried out or that the combined process would have a likelihood of success.

Moreover, the Squilla-Merkle combination fails to teach each and every claim limitation. Claim 4 recites visually comparing the signed hardcopy document with a printed hardcopy document of the authenticated lossy compressed image data. In contrast, Merkle teaches a signing copier for printing a hardcopy document based on the information located in the digital signature (Merkle, Col. 5, lines 36-45; Col. 8, lines 3-6). The signed hardcopy document is scanned and digitized by the signing copier, and the digital signature is processed via a checking algorithm (Merkle, Col. 3, lines 61-67). The checking algorithm determines whether the digital signature corresponds to the original hardcopy document (Merkle, Col. 3, line 67-Col. 4, line 10). The copier can display a

message indicating successful authentication or alternatively, the message can be printed directly on the digitally cleaned hardcopy document (Merkle, Col. 6, line 67-Col. 7, line 12). Additionally, the signing copier can be programmed not to make hardcopies of the signed document unless the signed document has been previously verified (Merkle, Col. 5, lines 53-59). Therefore, Merkle teaches a signing copier for authenticating a hardcopy document, rather than visually comparing the signed hardcopy document with a printed hardcopy document of the authenticated lossy compressed image data, per Claim 4.

Accordingly, the Squilla-Merkle combination fails to teach each and every limitation and a *prima facie* case of obviousness under 35 U.S.C. § 103(a) has not been shown. The rejection cannot be sustained and should be withdrawn.

C. U.S. Patent No. 5,946,103 ("Curry")

Applicant continues to assert that the Squilla-Curry combination fails to disclose, teach, or suggest all the limitations of Claims 6 and 9-11 based on the patentability of Claim 1. Accordingly, the rejection under 35 U.S.C. § 103(a) cannot be sustained and should be withdrawn.

D. U.S. Patent No. 5,486,686 ("Zdybel")

Applicant asserts that the Squilla and Zdybel references are being improperly combined, and the combination fails to disclose, teach, or suggest all the limitations of Claims 14-17.

The teachings of Squilla are discussed above with reference to the rejection under 35 U.S.C. § 102(e). Zdybel teaches a data recognition and recovery system using a lossless communications medium (Zdybel, Abstract; Col. 4, lines 20-41). A hardcopy document is scanned to create an electronic bitmap (Zdybel, Col. 7, lines 62-66), which is encoded into glyph encodings for printing on a hardcopy document (Zdybel, Col. 8, lines 38-50). The complete electronic document or a portion of the document can be selected for printing on the hardcopy output document and utilized in lieu of the recognition software for uploading a copy of the electronic document from the hardcopy document (Zdybel, Col. 9, lines 38-45).

One of ordinary skill in the art would not find a motivation to modify or combine Squilla with Zdybel. As described above, Squilla teaches an authentication system for digital images using a select portion of each image (Squilla, Col. 4, lines 13-15). In contrast, Zdybel teaches a data recovery system using glyph encodings printed on a hardcopy document (Zdybel, Col. 8, lines 38-50). The glyph encodings are not encoded or intended to provide authentication of the underlying hardcopy document. Rather, the glyph encodings represent the digital data content of ASCII, DDL or PDL encodings, which are determined by using recognition software to extract semantic information in the form of bit-level digital data contents from a document (Zdybel, Col. 7, line 66-Col. 8, line 4). Therefore, since Squilla teaches an authentication system and Zdybel teaches a data recognition and recovery system, the references are not in the same field of endeavor, and there is no suggestion to combine the references.

Further, the Squilla-Zdybel combination fails to teach each and every limitation of Claims 14-17. Claim 14 recites recording exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document. Claim 15 recites recording the location of exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document. A document is compressed by identifying tokens that are identical or nearly identical with a single exemplar (Spec., p. 14, lines 4-9). For example, two instances of the letter "e" in the same font and same font size can be recorded by one exemplar (Spec., p. 14, lines 6-7).

In contrast, Zdybel teaches an electronic document consisting of a bitmap, which is converted into textual encodings (Zdybel, Col. 7, lines 62-66). All or a portion of the textual encodings are converted into glyphs and printed onto a hardcopy output document (Zdybel, Col. 9, lines 38-41). An exemplar differs from the encodings of Zdybel, which include all the textual and appearance related data in a selected area (Zdybel, Col. 9, lines 38-58). Conversely, exemplars are groupings of data collected throughout a document. An exemplar does not require all or a portion of the textual and appearance related data, but rather, information selected from anywhere in the document that contains

identical or nearly identical tokens (Spec., p. 14, lines 4-9). Zdybel teaches combining hardcopy output and electronic documents into a lossless communications medium for recovering textual and appearance related data (Zdybel, Abstract; Col. 4, lines 20-41), rather than compressing data using exemplars, per Claims 14 and 15. Moreover, the Squilla-Zdybel combination fails to teach each and every limitation of Claims 14-17 based on the patentability of Claim 1.

Accordingly, a *prima facie* case of obviousness under 35 U.S.C. § 103(a) has not been shown. The rejection cannot be sustained and should be withdrawn.

E. U.S. Patent No. 6,111,953 ("Walker")

Applicant continues to assert that the Squilla and Walker references are being improperly combined, and the combination fails to disclose, teach, or suggest all the limitations of Claims 18-20.

Claim 18 recites an authentication token including encrypted image data or hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data. In contrast, Squilla teaches compressing a selected region of a digital image, hashing the compressed region, and encrypting the hash to generate a digital signature (Squilla, Col. 8, lines 34-51). The digital signature includes the hashed region of interest and photographer's information, such as the date and time of the photograph, which is attached to the hashed region of interest (Squilla, Col. 7, lines 31-34; Col. 8, lines 34-51). Further, Squilla teaches an authentication system that resolves the problem of using large amounts of battery power in a digital camera during image authentication (Squilla, Col. 2, lines 44-56). Creating an authentication token including both the compressed image data and a hash of the compressed image data requires more battery power and is contrary to the teachings of Squilla. Therefore, the Squilla-Walker combination fails to teach or suggest an authentication token including both the compressed image data and a hash of the compressed image data. The combination further fails to teach an authentication token containing only encrypted image data.

Accordingly, a *prima facie* case of obviousness under 35 U.S.C. § 103(a)

has not been shown. The rejection under 35 U.S.C. § 103(a) cannot be sustained and should be withdrawn.

Reconsideration of the pending claims and a Notice of Allowance are respectfully solicited. Appellant's undersigned attorney can be reached at (206) 381-3900.

Dated: May 2, 2007

By: Krista
Krista A. Wittman, Esq.
Reg. No. 59,594

Cascadia Intellectual Property
500 Union Street
Suite 1005
Seattle, WA 98101

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

4. CLAIMS APPENDIX

1. (previously presented): A method for authenticating a hardcopy document, comprising the steps of:

recording in a memory a scanned representation of the hardcopy document at a selected resolution;

generating lossy compressed image data with the scanned representation of the hardcopy document;

producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

arranging in the memory the scanned representation of the hardcopy document with a digital encoding of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

2. (original): The method according to claim 1, further comprising the step of verifying the signed hardcopy document by:

recording a scanned representation of the signed hardcopy document;

decoding the authentication token from the scanned representation of the signed hardcopy document;

authenticating the lossy compressed image data using one of the encrypted image data and the hashed encrypted image data; and

decompressing the authenticated lossy compressed image data for comparison with the signed hardcopy document to determine whether the signed hardcopy document is authentic.

3. (original): The method according to claim 2, further comprising the step of visually comparing the signed hardcopy document with the authenticated lossy compressed image data.

4. (original): The method according to claim 2, further comprising the step of visually comparing the signed hardcopy document with a printed hardcopy document of the authenticated lossy compressed image data.

5. (original): The method according to claim 2, wherein said step of producing an authentication token is performed with a private key and said step of authenticating lossy compressed image data is performed with a public key.

6. (original): The method according to claim 1, further comprising the step of encoding the authentication token in a low intensity background pattern.

7. (original): The method according to claim 1, further comprising the step of encoding the authentication token in embedded data.

8. (original): The method according to claim 7, wherein said encoding step encodes the authentication token in a halftone pattern.

9. (original): The method according to claim 8, wherein said encoding step encodes the authentication token in a hyperbolic halftone pattern.

10. (original): The method according to claim 8, wherein said encoding step encodes the authentication token in a serpentine halftone pattern.

11. (original): The method according to claim 7, wherein said encoding step encodes the authentication token in data glyphs.

12. (original): The method according to claim 1, wherein said step of generating lossy compressed image data loses document formatting contained in the scanned representation of the hardcopy document.

13. (original): The method according to claim 12, wherein said step of generating lossy compressed image data further comprises the step of compressing the scanned representation of the hardcopy document by identifying exemplars and locations of exemplars; each exemplar identified representing one

or more image segments from the scanned representation of the hardcopy document.

14. (original): The method according to claim 13, wherein said compressing step records the exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document.

15. (original): The method according to claim 13, wherein said compressing step records that locations of exemplars at a resolution that is less than the selected resolution of the scanned representation of the hardcopy document.

16. (original): The method according to claim 1, wherein said compressing step compresses identified portions of the image data at a plurality of compression ratios.

17. (original): The method according to claim 16, further comprising the step of segmenting text data from pictorial data before compressing the scanned representation of the hardcopy document.

18. (original): A method for authenticating a hardcopy document, comprising the steps of:

recording in a memory a scanned representation of the hardcopy document at a selected resolution;

generating lossy compressed image data with the scanned representation of the hardcopy document;

producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

arranging in the memory a digital encoding of the authentication data for rendering at a printer a label containing the digital encoding of the authentication data.

19. (original): The method according to claim 18, further comprising the step of fixedly attaching the label to the hardcopy document to produce a signed hardcopy document.

20. (original): The method according to claim 19, further comprising the step of verifying the signed hardcopy document by:

recording a scanned representation of the signed hardcopy document;

decoding the authentication token from the scanned representation of the signed hardcopy document;

authenticating the lossy compressed image data using one of the encrypted image data and the hashed encrypted image data; and

decompressing the authenticated lossy compressed image data for comparison with the signed hardcopy document to determine whether the signed hardcopy document is authentic.

21. (previously presented): A system for authenticating a scanned representation of a hardcopy document, comprising:

an image compression module for generating lossy compressed image data with the scanned representation of the hardcopy document;

an authentication token generator for producing an authentication token with the lossy compressed image data; the authentication token including one of encrypted image data and hashed encrypted image data; the hashed encrypted image data including the lossy compressed image data and an encrypted hash of the lossy compressed image data; and

an encoding module for arranging the scanned representation of the hardcopy document with a digital encoding of the authentication token for rendering at a printer a signed and authenticated hardcopy document.

22. (previously presented): The system according to Claim 21, further comprising:

a memory for recording the signed hardcopy document;

a decoding module for decoding the signed hardcopy document to define decoded signed image data;

an authentication module to authenticating the decided signed image data using of the encrypted image data and the hashed encrypted image data to define authenticated image data; and

a decompression module for decompressing the authenticated image data to define decompressed image data;

means for comparing the signed hardcopy document with the authenticated hardcopy document to determine whether the signed hardcopy document is authentic.

23. (previously presented): The system according to Claim 21, wherein said image compression module compresses the scanned representation of the hardcopy document by identifying exemplars and locations of exemplars; each exemplar identified representing one or more image segments from the scanned representation of the hardcopy document.

5. EVIDENCE APPENDIX

None.

6. RELATED PROCEEDINGS APPENDIX

None.